Patent
Attorney's Docket No. 009683-470

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Patent Application of | ) | |
| | ) | |
| Shuzo FUJIOKA | ) | Group Art Unit: Unassigned |
| | ) | |
| Application No.: Unassigned | ) | Examiner: Unassigned |
| | ) | |
| Filed: July 10, 2003 | ) | Confirmation No.: Unassigned |
| | ) | |
| For: INFORMATION SECURITY MICROCOMPUTER HAVING AN INFORMATION SECURITY FUNCTION AND AUTHENTICATING AN EXTERNAL DEVICE | ) | |

**CLAIM FOR CONVENTION PRIORITY**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japan Patent Application No. 2002-380316
Filed: December 27, 2002

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 10, 2003

By: _____
Platon N. Mandros
Registration No. 22,124

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

(05/03)

# 日　本　国　特　許　庁
## JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１２月２７日

出願番号
Application Number:　特願２００２－３８０３１６

[ST.10/C]:　[ＪＰ２００２－３８０３１６]

出願人
Applicant(s):　三菱電機株式会社
三菱電機システムエル・エス・アイ・デザイン株式会社

２００３年　１月３１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３００３０３１

【書類名】　特許願
【整理番号】　541256JP01
【提出日】　平成14年12月27日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/14
G06F 15/78
【発明者】
【住所又は居所】　兵庫県伊丹市中央３丁目１番１７号　三菱電機システムエル・エス・アイ・デザイン株式会社内
【氏名】　藤岡　宗三
【特許出願人】
【識別番号】　000006013
【氏名又は名称】　三菱電機株式会社
【特許出願人】
【識別番号】　391024515
【氏名又は名称】　三菱電機システムエル・エス・アイ・デザイン株式会社
【代理人】
【識別番号】　100064746
【弁理士】
【氏名又は名称】　深見　久郎
【選任した代理人】
【識別番号】　100085132
【弁理士】
【氏名又は名称】　森田　俊雄
【選任した代理人】
【識別番号】　100083703
【弁理士】
【氏名又は名称】　仲村　義平

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100098316

【弁理士】

【氏名又は名称】　野田　久登

【選任した代理人】

【識別番号】　100109162

【弁理士】

【氏名又は名称】　酒井　將行

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　情報セキュリティマイクロコンピュータ、そのプログラム開発装置およびそれらを含んだプログラム開発システム

【特許請求の範囲】

【請求項１】　情報セキュリティ機能を有する情報セキュリティマイクロコンピュータであって、

情報の暗号化および復号を行なうための暗号手段と、

外部機器の認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、情報セキュリティマイクロコンピュータ。

【請求項２】　前記プロセッサは、乱数を発生させて前記外部機器へ送信し、前記外部機器から受信した情報を復号し、該復号された値が前記乱数と一致するか否かを判定して前記外部機器の認証を行なう、請求項１記載の情報セキュリティマイクロコンピュータ。

【請求項３】　前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータ全体の動作を停止させる、請求項１または２記載の情報セキュリティマイクロコンピュータ。

【請求項４】　前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記暗号手段の動作を停止させる、請求項１または２記載の情報セキュリティマイクロコンピュータ。

【請求項５】　前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記暗号手段による演算結果を正しく出力しないようにする、請求項１または２記載の情報セキュリティマイクロコンピュータ。

【請求項６】　前記プロセッサは、デバッグモードおよび一般モードのいずれかで動作し、

前記情報セキュリティマイクロコンピュータはさらに、デバッグモードに固定するためのモードロック手段を含む、請求項１～５のいずれかに記載の情報セキ

ユリティマイクロコンピュータ。

【請求項７】　情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、前記情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体とを含んだプログラム開発装置であって、

前記本体は、前記情報セキュリティマイクロコンピュータとの認証を行ない、コマンドを発行して前記情報セキュリティマイクロコンピュータを制御するための制御手段を含み、

前記情報セキュリティマイクロコンピュータは、前記本体との認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、プログラム開発装置。

【請求項８】　情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、

前記情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体と、

前記本体を介して前記情報セキュリティマイクロコンピュータにコマンドを発行するコンピュータとを含み、

前記情報セキュリティマイクロコンピュータ、前記本体および前記コンピュータのうち、少なくともいずれか２つの間で認証を行なう、プログラム開発システム。

【請求項９】　前記情報セキュリティマイクロコンピュータは、情報の暗号化および復号を行なうための暗号手段と、

前記本体または前記コンピュータの認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、請求項８記載のプログラム開発システム。

【請求項１０】　前記情報セキュリティマイクロコンピュータ、前記本体および前記コンピュータのうち、少なくともいずれか２つの間で行なわれる認証は、一定時間毎に繰返し行なわれる、請求項８または９記載のプログラム開発システム。

【請求項１１】　前記本体は、前記コンピュータとの認証を行ない、認証が確認されなかった場合には前記本体の少なくとも一部の機能が動作しないように制御する、請求項８～１０のいずれかに記載のプログラム開発システム。

【請求項１２】　前記本体は、前記コンピュータとの認証を行なうと共に、前記情報セキュリティマイクロコンピュータとの認証を行ない、いずれかの認証が確認されなかった場合には前記情報セキュリティマイクロコンピュータまたは本体の少なくとも一部の機能が動作しないように制御を行なう、請求項８～１０のいずれかに記載のプログラム開発システム。

【請求項１３】　前記コンピュータは、利用者からの認証情報を受けて前記情報セキュリティマイクロコンピュータに送信し、

前記情報セキュリティマイクロコンピュータは、前記コンピュータから受信した認証情報が予め保持する認証情報と一致するか否かを判定し、

前記コンピュータは、前記情報セキュリティマイクロコンピュータによって認証情報が一致しないと判定された場合には、前記本体の少なくとも一部の機能が動作しないように制御する、請求項８～１２のいずれかに記載のプログラム開発システム。

【請求項１４】　前記コンピュータは、利用者による入力が一定時間以上なかった場合には、利用者に対して再度認証情報を入力させる、請求項１３記載のプログラム開発システム。

【請求項１５】　前記プログラム開発システムはさらに、前記コンピュータと前記本体とを接続するネットワークを含み、

前記コンピュータは、前記本体にプログラムをダウンロードするときに、当該プログラムを暗号化して送信し、

前記本体は、前記コンピュータから受信した前記暗号化されたプログラムを復号して実行する、請求項８～１０のいずれかに記載のプログラム開発システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ機能を搭載したマイクロコンピュータ（以下、情報セキュリティマイコンと略す。）に関し、特に、インサーキットエミュレータ（以下、ＩＣＥと略す。）に使用される情報セキュリティマイコン、そのプログラム開発装置およびそれらを含んだプログラム開発システムに関する。

【０００２】

【従来の技術】

近年、ユーザの正当性の確認や情報の漏洩の防止などに情報セキュリティが広く用いられており、情報セキュリティ機能を搭載したマイコンの開発も進んできている。このような情報セキュリティマイコンにおいても、一般のマイコンと同様にプログラム開発時にＩＣＥを用いてデバッグが行なわれる。

【０００３】

ＩＣＥ本体は、パーソナルコンピュータ（以下、ＰＣと略す。）との接続に使用されるホストインタフェースや、ＩＣＥ用マイコンとの接続に使用されるＩＣＥインタフェースを有しており、さらにＩＣＥ全体の制御を行なう機能も有しているものもある。

【０００４】

ＩＣＥ本体は、ＰＣからの命令によって、ＩＣＥ用マイコンに対するプログラムの実行、ターゲットボードに搭載されたメモリの内容のダンプ、プログラムを１命令ずつ実行させるステップ実行、プログラムを所定の番地で停止させるブレークなどの機能を実現する。これに関連する技術として、特開２０００－３４７９４２号公報に開示された発明がある。

【０００５】

特開２０００－３４７９４２号公報に開示された情報処理装置においては、ＲＯＭ（Read Only Memory）に記憶された情報を外部に設けられたデバッグツールによる不正アクセスから保護するものであり、予め登録されたコードと外部から与えられたパスワードとを照合し、両者が一致した場合にはオンチップデバッグ

回路の機能を有効にするものである。

【０００６】

【特許文献１】

特開２０００－３４７９４２号公報

【０００７】

【発明が解決しようとする課題】

上述したＩＣＥは、本来マイコンのプログラム開発に利用されるものであるが、悪用されるとリバースエンジニアリング、プログラムの解析、情報の改ざんなどが可能になるといった問題点があった。

【０００８】

また、従来のＩＣＥは、接続の権限がない外部機器を接続しても動作するため、悪意を有する者がＩＣＥを利用して情報セキュリティマイコンを搭載したシステムを解析したり、情報セキュリティマイコンを偽造したりすることが可能になるといった問題点があった。

【０００９】

また、ＩＣＥ用マイコンは、プログラム開発の対象である情報セキュリティマイコンと同じ機能と、ＩＣＥ本体からの制御を可能にするＩＣＥインタフェースとを有しており、情報セキュリティマイコンの代わりにＩＣＥ用マイコンをシステムボードに載せることによって、システムの偽造に利用されたり、対象である情報セキュリティマイコンの解析に利用されたりするといった問題点があった。

【００１０】

また、ＩＣＥに接続されるＰＣには、情報セキュリティマイコンが実行するプログラムなどのセキュリティ情報が格納されており、誰でもそのＰＣを利用できるとプログラムが盗まれるといった問題点があった。

【００１１】

また、ＰＣおよびＩＣＥをネットワークに接続したシステムにおいては、ＩＣＥを用いてプログラムをデバッグする場合、プログラムをＰＣからＩＣＥにダウンロードするため、その情報が傍受されてプログラムが盗用される可能性があるといった問題点があった。

【００１２】

さらには、上述した特開２０００－３４７９４２号公報に開示された情報処理装置においては、予め登録されたコードと外部から与えられたパスワードとを照合し、両者が一致した場合にはオンチップデバッグ回路の機能を有効にしてＲＯＭに対する不正アクセスを防止するものであるが、パスワードを入力すれば接続の権限がない外部機器であってもＲＯＭの内容を読出すことができるため、セキュリティの強化を図ることができない。

【００１３】

本発明は、上記問題点を解決するためになされたものであり、その目的は、使用権限がない者がＩＣＥ用マイコンとして利用することが不可能な情報セキュリティマイクロコンピュータを提供することである。

【００１４】

【課題を解決するための手段】

本発明のある局面に従えば、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータであって、情報の暗号化および復号を行なうための暗号手段と、外部機器の認証を行なうための認証手段と、情報セキュリティマイクロコンピュータの全体的な制御を行ない、認証手段によって認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む。

【００１５】

本発明の別の局面に従えば、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体とを含んだプログラム開発装置であって、本体は、情報セキュリティマイクロコンピュータとの認証を行ない、コマンドを発行して情報セキュリティマイクロコンピュータを制御するための制御手段を含み、情報セキュリティマイクロコンピュータは、本体との認証を行なうための認証手段と、情報セキュリティマイクロコンピュータの全体的な制御を行ない、認証手段によって認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む。

【００１６】

本発明のさらに別の局面に従えば、プログラム開発システムは、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体と、本体を介して情報セキュリティマイクロコンピュータにコマンドを発行するコンピュータとを含み、情報セキュリティマイクロコンピュータ、本体およびコンピュータのうち、少なくともいずれか２つの間で認証を行なう。

【００１７】

【発明の実施の形態】

（第１の実施の形態）

図１は、本発明の第１の実施の形態におけるＩＣＥ用マイコンの概略構成を示すブロック図である。このＩＣＥ用マイコン１は、ＩＣＥ用マイコン全体の制御を行なうＣＰＵ（Central Processing Unit）１１と、プログラムやデータを記憶するメモリ１２と、認証データなどが格納される不揮発メモリ１３と、外部機器との通信を行なう通信回路１４と、ＩＣＥ本体と通信を行なうＩＣＥインタフェース１５と、所定のデータを認証データによって暗号化および復号を行ない、乱数を発生させる暗号回路１６と、ＩＣＥ本体との間の認証を行なう認証用プログラム１７とを含む。

【００１８】

暗号回路１６は、不揮発メモリ１３に格納された認証データを参照して暗号化および復号を行なうプログラムを、ＣＰＵ１１が実行することによって実現される。また、ＣＰＵ１１が認証用プログラム１７を実行することによって、ＩＣＥ本体の認証が行なわれる。この認証用プログラム１７は、メモリ１２に格納されていてもよい。

【００１９】

図２は、ＩＣＥ用マイコン１とＩＣＥ本体との間の認証を説明するための図である。図２においては、認証の一例としてチャレンジ＆レスポンス方式の認証を示しており、共通鍵暗号方式を利用した場合を示している。ＩＣＥ用マイコン１とＩＣＥ本体とに、予め同じ暗号鍵が認証データとして格納されているものとす

る。なお、共通鍵暗号方式ではなく、公開鍵暗号方式を用いてもよい。

【００２０】

まず、ＩＣＥ用マイコン１（認証する側）内のＣＰＵ１１は、認証用プログラム１７を実行することによって乱数を発生させ、生成した乱数をＩＣＥインタフェース１５を介してＩＣＥ本体（認証される側）へ送信する。

【００２１】

ＩＣＥ本体は、ＩＣＥ用マイコン１から乱数を受信し、この乱数を予め格納している認証データを用いて暗号化する。そして、ＩＣＥ本体は、この暗号化した乱数をＩＣＥ用マイコン１へ送信する。

【００２２】

ＩＣＥ用マイコン１は、ＩＣＥ本体から暗号化された乱数を受信し、不揮発メモリ１３に予め格納される認証データを用いてそれを復号する。そして、復号された値が自身が生成した乱数と一致する場合には、ＩＣＥ本体の認証が確認されたものとする。また、復号された値が自身が生成した乱数と一致しない場合には、ＩＣＥ本体の認証が確認されなかったものとする。

【００２３】

図３は、本発明の第１の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの一例を示す図である。このプログラム開発システムは、ＩＣＥ２と、ＩＣＥ２に接続されるＰＣ３と、ターゲットボード４とを含む。また、ＩＣＥ２は、ＩＣＥ本体２１と、ＩＣＥ用マイコン１が搭載されるＰＯＤ２２とを含む。ＰＯＤ２２は、ターゲットボード４に接続される。

【００２４】

ＰＣ３は、ＩＣＥ２に対して命令を送信することによって、ＩＣＥ用マイコン１に対するプログラムの実行、ターゲットボード４に搭載されたメモリの内容のダンプ、プログラムを１命令ずつ実行させるステップ実行、プログラムを所定の番地で停止させるブレークなどの機能を実現する。

【００２５】

図４は、ＩＣＥ２の機能的構成を示すブロック図である。ＩＣＥ２は、ＩＣＥ２の全体的な制御を行なうＩＣＥ制御部（ＩＣＥ本体）２１と、ＩＣＥ用マイコ

ン１が搭載されるＰＯＤ２２とを含む。

【００２６】

ＩＣＥ制御部２１は、予め認証データを保持しており、ＩＣＥ用マイコン１から乱数を受信すると、認証データを用いて乱数を暗号化してＩＣＥ用マイコン１へ送信する。また、ＩＣＥ制御部２１は、ＰＣ３から命令を受信すると、その命令をＰＯＤ２２に搭載されたＩＣＥ用マイコン１へ送信する。

【００２７】

図５は、本発明の第１の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。まず、ＰＯＤ２２に搭載されたＩＣＥ用マイコン１が動作を開始すると、ＣＰＵ１１は乱数を発生させ（Ｓ１１）、その乱数をＩＣＥインタフェース１５を介してＩＣＥ本体２１へ送信する（Ｓ１２）。

【００２８】

ＩＣＥ本体２１は、ＩＣＥ用マイコン１から乱数を受信すると（Ｓ１３）、予め保持している認証データを暗号鍵として用い、受信した乱数を暗号化する。そして、ＩＣＥ本体２１は、暗号化した乱数をＩＣＥ用マイコン１へ送信する（Ｓ１４）。

【００２９】

ＩＣＥ用マイコン１は、ＩＣＥ本体２１から暗号化された乱数を受信すると（Ｓ１５）、予め不揮発メモリ１３に保持している認証データを復号鍵として用い、受信した暗号化された乱数を復号する（Ｓ１６）。そして、ＩＣＥ用マイコン１は、復号した値と自身が生成した乱数とを比較する（Ｓ１７）。

【００３０】

復号した値と自身が生成した乱数とが一致しない場合には（Ｓ１８，Ｙｅｓ）、ＩＣＥ用マイコン１全体の動作を停止させる（Ｓ１９）。また、復号した値と自身が生成した乱数とが一致する場合には（Ｓ１８，Ｎｏ）、ＩＣＥ機能の動作を開始する（Ｓ２０）。

【００３１】

ＩＣＥ本体２１がＩＣＥ用マイコン１に対してコマンドを送信すると（Ｓ２１

）、ＩＣＥ用マイコン１はコマンドを受信し（Ｓ２２）、当該コマンドを実行する（Ｓ２３）。そして、ＩＣＥ用マイコン１はコマンドの実行結果をＩＣＥ本体２１へ送信する（Ｓ２４）。ＩＣＥ本体２１は、ＩＣＥ用マイコン１からコマンドの実行結果を受信すると（Ｓ２５）、その実行結果をＰＣ３へ送信して、ＰＣ３から次の命令を受信するまで待機する。

【００３２】

以上の説明においては、ＩＣＥ用マイコン１がＩＣＥ本体２１の認証を行なうものであったが、ＩＣＥ本体２１がＩＣＥ用マイコン１の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【００３３】

以上説明したように、本実施の形態におけるＩＣＥ用マイコン１によれば、ＩＣＥ本体２１の認証を行ない、認証が確認された場合にはＩＣＥ機能の動作を行ない、認証が確認されなかった場合にはＩＣＥ用マイコン１の動作を停止するようにしたので、悪意のある者が別のシステムでそのＩＣＥ用マイコンを利用することができなくなり、セキュリティを向上させることが可能となった。

【００３４】

（第２の実施の形態）

本発明の第１の実施の形態におけるＩＣＥ用マイコン１においては、認証が確認されなかった場合にはＩＣＥ用マイコン１の動作を全て停止させるものであったが、第２の実施の形態におけるＩＣＥ用マイコン１は認証が確認されなかった場合にはＩＣＥ用マイコン１内の暗号回路１６の動作のみを停止させるものである。

【００３５】

本発明の第２の実施の形態におけるＩＣＥ用マイコンは、図１に示す第１の実施の形態におけるＩＣＥ用マイコンと比較して、ＩＣＥ本体２１の認証が確認されなかった場合には暗号回路１６の動作のみが停止される点を除いて同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００３６】

図６は、本発明の第２の実施の形態におけるＩＣＥ用マイコン１を用いたプロ

グラム開発システムの処理手順を説明するためのフローチャートである。図５に示す第１の実施の形態におけるプログラム開発システムの処理手順と比較して、ステップＳ１９の処理のみが異なる。したがって、重複する処理手順の詳細な説明は省略する。なお、本実施の形態におけるステップＳ１９の参照符号をＳ１９’として説明する。

【００３７】

ステップＳ１８において、復号した値と自身が生成した乱数とが一致しない場合には（Ｓ１８，Ｙｅｓ）、ＩＣＥ用マイコン１内の暗号回路１６の動作のみを停止させる（Ｓ１９’）。また、復号した値と自身が生成した乱数とが一致する場合には（Ｓ１８，Ｎｏ）、ＩＣＥ機能の動作を開始する（Ｓ２０）。

【００３８】

一般に、セキュリティに関係するデバッグは、暗号回路１６を利用したプログラムに集中するため、セキュリティに関するプログラムのデバッグを行なう者のみに暗号回路１６の使用を認め、それ以外の者には暗号回路１６の使用を認めないようにすることができる。たとえば、ＰＣの起動時にＩＣＥ２に利用者認証を要求し、ＩＣＥ本体２１がＩＣＥ用マイコン１との認証を行なうようにする。そして、認証が確認されれば、暗号回路１６を含んだＩＣＥ用マイコン１全体の動作を認め、認証が確認されなければ、暗号回路１６の動作のみを停止してそれ以外の動作を認める。

【００３９】

以上説明したように、本実施の形態におけるＩＣＥ用マイコン１によれば、ＩＣＥ本体２１の認証を行ない、認証が確認された場合にはＩＣＥ機能の動作を行ない、認証が確認されなかった場合にはＩＣＥ用マイコン１内の暗号回路１６の動作のみを停止するようにしたので、利用権限を有する開発者のみが暗号回路１６を利用したデバッグを行なえ、利用権限を有しない開発者には暗号回路１６を利用しないデバッグのみを行えるようにするといった、役割分担に応じたプログラム開発が可能になった。

【００４０】

（第３の実施の形態）

本発明の第１の実施の形態におけるＩＣＥ用マイコン１においては、認証が確認されなかった場合にはＩＣＥ用マイコン１の動作を全て停止させるものであったが、第３の実施の形態におけるＩＣＥ用マイコン１は認証が確認されなかった場合にはＩＣＥ用マイコン１内の暗号回路１６が正しい演算結果を出力しないようにしたものである。

【００４１】

本発明の第３の実施の形態におけるＩＣＥ用マイコンは、図１に示す第１の実施の形態におけるＩＣＥ用マイコンと比較して、ＩＣＥ本体２１の認証が確認されなかった場合には暗号回路１６が正しい演算結果を出力しない点を除いて同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４２】

図７は、本発明の第３の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。図５に示す第１の実施の形態におけるプログラム開発システムの処理手順と比較して、ステップＳ１９の処理のみが異なる。したがって、重複する処理手順の詳細な説明は省略する。なお、本実施の形態におけるステップＳ１９の参照符号をＳ１９”として説明する。

【００４３】

ステップＳ１８において、復号した値と自身が生成した乱数とが一致しない場合には（Ｓ１８，Ｙｅｓ）、ＩＣＥ用マイコン１内の暗号回路１６が正しい演算結果を出力しない（Ｓ１９”）。また、復号した値と自身が生成した乱数とが一致する場合には（Ｓ１８，Ｎｏ）、ＩＣＥ機能の動作を開始する（Ｓ２０）。なお、復号した値と自身が生成した乱数とが一致しない場合には、演算結果を全く出力しないようにしてもよい。

【００４４】

一般に、セキュリティに関係するデバッグは、暗号回路１６を利用したプログラムに集中するため、セキュリティに関するプログラムのデバッグを行なう者のみに暗号回路１６の使用を認め、それ以外の者には暗号回路１６の使用を認めるがセキュリティ情報の確認を行なえないようにすることができる。たとえば、Ｐ

Ｃの起動時にＩＣＥ２に利用者認証を要求し、ＩＣＥ本体２１がＩＣＥ用マイコン１との認証を行なうようにする。そして、認証が確認されれば、暗号回路１６を含んだＩＣＥ用マイコン１全体の動作を認め、認証が確認されなければ、暗号回路１６が正しい演算結果を出力しないように動作し、それ以外のＩＣＥ用マイコン１の動作を認める。

【００４５】

以上説明したように、本実施の形態におけるＩＣＥ用マイコン１によれば、ＩＣＥ本体２１の認証を行ない、認証が確認された場合にはＩＣＥ機能の動作を行ない、認証が確認されなかった場合にはＩＣＥ用マイコン１内の暗号回路１６が正しい演算結果を出力しないようにしたので、利用権限を有する開発者のみが暗号回路１６を利用したデバッグを行なえ、利用権限を有しない開発者は暗号回路１６の機能的な検証は行なえるが、セキュリティ情報の確認を行なうことができないといった、役割分担に応じたプログラム開発が可能になった。

【００４６】

（第４の実施の形態）

本発明の第４の実施の形態におけるプログラム開発システムの概略構成は、図３に示す第１の実施の形態におけるプログラム開発システムの概略構成と同様である。また、本発明の第４の実施の形態におけるＩＣＥ２の機能的構成は、図４に示す第１の実施の形態におけるＩＣＥ２の機能的構成と同様である。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４７】

図８は、本発明の第４の実施の形態におけるＩＣＥ本体２１の機能的構成を示すブロック図である。ＩＣＥ本体２１は、ＩＣＥ本体２１の全体的な制御を行なうＩＣＥ制御部２１１と、認証用プログラム２１２と、認証データ２１３とを含む。

【００４８】

ＩＣＥ制御部２１１は、ＰＣ３との間で通信を行なうホストインタフェースと、ＩＣＥ用マイコン１との間で通信を行なうＩＣＥインタフェースとを有している。ＩＣＥ制御部２１１は、ホストインタフェースを介してＰＣ３からコマンド

を受信すると、ＩＣＥ用マイコン１にそのコマンドを送信する。ＩＣＥ用制御部２１１は、ＩＣＥ用マイコン１からそのコマンドの実行結果を受信すると、実行結果をＰＣ３へ送信する。このようにして、ＰＣ３はＩＣＥマイコン１の動作を制御することが可能になる。

【００４９】

ＩＣＥ本体２１は、ＩＣＥ用マイコン１に格納される認証データと同じ認証データ２１３を有しており、認証用プログラム２１２は、認証データ２１３を用いてＩＣＥ用マイコン１と同様の認証を行なう。ＩＣＥ用マイコン１の認証が確認されなかった場合のＩＣＥ用マイコン１の動作は、図５～図７を用いて説明した第１～第３の実施の形態におけるＩＣＥ用マイコン１の動作と同様である。

【００５０】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＩＣＥ本体２１がＩＣＥ用マイコン１の認証を行なうようにしたので、認証機能を持たないＩＣＥ本体２１はＩＣＥ用マイコン１を用いてデバッグ等を行なえなくなり、セキュリティを向上させることが可能となった。

【００５１】

（第５の実施の形態）

図９は、本発明の第５の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ＩＣＥ本体２１と、ＰＯＤ２２と、ターゲットボード４とを含む。ＰＣ３は、認証用プログラムおよび認証データを格納しており、ＩＣＥ用マイコン１がＰＣ３の認証を行なう。ＰＣ３の認証が確認されなかった場合のＩＣＥ用マイコン１の動作は、図５～図７を用いて説明した第１～第３の実施の形態におけるＩＣＥ用マイコン１の動作と同様である。

【００５２】

図１０は、本発明の第５の実施の形態におけるプログラム開発システムの概略構成の他の一例を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ＰＯＤ２２と、ターゲットボード４とを含む。ＰＣ３は、ＩＣＥ本体２１が有する機能を有しており、ＰＣ３が直接ＰＯＤ２２内のＩＣＥ用マイコン１と

通信を行なうことにより、ＩＣＥ用マイコン１がＰＣ３の認証を行なう。

【００５３】

以上の説明においては、ＩＣＥ用マイコン１がＰＣ３の認証を行なうものであったが、ＰＣ３がＩＣＥ用マイコン１の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【００５４】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＩＣＥ用マイコン１とＰＣ３との間で認証を行なうようにしたので、ＩＣＥ用マイコン１を利用する権限のないＰＣ３はＩＣＥ用マイコン１を動作させることができないため、セキュリティを向上させることが可能となった。また、ＰＣ３以外の計測機器を接続した場合でも、ＩＣＥ用マイコン１との間の認証が行なわれないので、ＩＣＥ用マイコン１の解析を防止することが可能となった。

【００５５】

（第６の実施の形態）

図１１は、本発明の第６の実施の形態におけるプログラム開発システムの概略構成を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ＩＣＥ本体２１と、ＰＯＤ２２と、ターゲットボード４とを含む。ＰＣ３は、認証用プログラムおよび認証データを格納している。また、ＩＣＥ本体２１も認証用プログラムおよび認証データを格納しており、ＩＣＥ本体２１がＰＣ３の認証を行なう。ＰＣ３の認証が確認されなかった場合のＩＣＥ用マイコン１の動作は、図５～図７を用いて説明した第１～第３の実施の形態におけるＩＣＥ用マイコン１の動作と同様である。

【００５６】

以上の説明においては、ＩＣＥ本体２１がＰＣ３の認証を行なうものであったが、ＰＣ３がＩＣＥ本体２１の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【００５７】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＩＣＥ本体２１とＰＣ３との間で認証を行なうようにしたので、ＩＣＥ本体２

１を利用する権限のないＰＣ３はＩＣＥ用マイコン１を動作させることができないため、セキュリティを向上させることが可能となった。また、ＰＣ３以外の計測機器を接続した場合でも、ＩＣＥ本体２１との間の認証が行なわれないので、ＩＣＥ用マイコン１の解析を防止することが可能となった。

【００５８】

（第７の実施の形態）

図１２は、本発明の第７の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ＩＣＥ本体２１と、ＰＯＤ２２と、ターゲットボード４とを含む。ＰＣ３は、認証用プログラムおよび認証データを格納している。また、ＩＣＥ本体２１も認証用プログラムおよび認証データを格納している。

【００５９】

ＩＣＥ用マイコン１とＩＣＥ本体２１との間で認証が行なわれると共に、ＩＣＥ本体２１とＰＣ３との間でも認証が行なわれる。ＩＣＥ用マイコン１とＩＣＥ本体２１との間の認証、およびＩＣＥ本体２１とＰＣ３との間の認証のいずれか、または両方の認証が確認されなかった場合のＩＣＥ用マイコン１の動作は、図５～図７を用いて説明した第１～第３の実施の形態におけるＩＣＥ用マイコン１の動作と同様である。

【００６０】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＩＣＥ用マイコン１とＩＣＥ本体２１との間、およびＩＣＥ本体２１とＰＣ３との間で認証を行なうようにしたので、ＩＣＥ用マイコン１を利用する権限のないＩＣＥ本体２１またはＰＣ３はＩＣＥ用マイコン１を動作させることができないため、さらにセキュリティを向上させることが可能となった。

【００６１】

（第８の実施の形態）

図１３は、本発明の第８の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ＩＣＥ本体２１と、ＰＯＤ２２と、ターゲットボード４とを含む。ＰＣ３は、

利用者によるパスワードの入力を受け、そのパスワードをＩＣＥ用マイコン１へ送信する。ＩＣＥ用マイコン１は、ＰＣ３から受信したパスワードと予め格納しているパスワードとを比較し、その比較結果をＰＣ３へ送信する。

【００６２】

図１４は、本発明の第８の実施の形態におけるプログラム開発システムの処理手順を説明するためのフローチャートである。まず、利用者がＰＣ３にパスワードを入力すると（Ｓ３１）、そのパスワードはＩＣＥ本体２１を介してＩＣＥ用マイコン１へ送信される。

【００６３】

ＩＣＥ用マイコン１は、ＰＣ３から受信したパスワードと、予め格納しているパスワードとを比較する（Ｓ３２）。パスワードが一致しなければ（Ｓ３２，Ｎｏ）、ＩＣＥ用マイコン１はＰＣ３へパスワードが一致しなかったことを通知する（Ｓ３３）。また、パスワードが一致すれば（Ｓ３２，Ｙｅｓ）、ＩＣＥ用マイコン１はＰＣ３へパスワードが一致したことを通知する（Ｓ３５）。

【００６４】

ＰＣ３は、ＩＣＥ用マイコン１からパスワードが一致しなかったことを示す通知を受けると、ＩＣＥ２を制御するプログラムを停止させるか、ＩＣＥ２の利用制限を行なう（Ｓ３４）。また、ＰＣ３は、ＩＣＥ用マイコン１からパスワードが一致したことを示す通知を受けると、ＰＣ３とＩＣＥ本体２１との認証を開始するか、ＩＣＥ本体２１とＩＣＥ用マイコン１との認証を行なうよう指示する（Ｓ３６）。

【００６５】

ＰＣ３とＩＣＥ本体２１との認証、またはＩＣＥ本体２１とＩＣＥ用マイコン１との認証が確認されれば（Ｓ３７，Ｎｏ）、ＩＣＥ２の起動を開始する（Ｓ３８）。また、ＰＣ３とＩＣＥ本体２１との認証、またはＩＣＥ本体２１とＩＣＥ用マイコン１との認証が確認されなければ（Ｓ３７，Ｙｅｓ）、ＩＣＥ２またはＩＣＥ用マイコン１の動作を停止させるか、ＩＣＥ２またはＩＣＥ用マイコン１の動作の制限を行なう（Ｓ３９）。

【００６６】

また、ＰＣ３は、利用者によるＰＣ３の操作が一定時間なかった場合には、画面をロックするようにしてもよい。この場合、利用者が再度パスワードを入力することにより、画面のロックが解除される。このようにして、利用権限を有する者がいない間に、利用権限を有しない者がＩＣＥ２を利用してプログラムのデバッグや解析を行なうことを防止することができる。

【００６７】

また、パスワードとＩＤとを用いて利用者を管理するようにすれば、利用者に役割分担に応じた利用権限を与えることができる。たとえば、利用者によって入力されたＩＤによって、ＩＣＥ用マイコン１が第１～第３の実施の形態において説明した動作制限のいずれかを選択して実行するようにすれば、ＩＤによってデバッグ可能なレベルを利用者毎に設定することができる。

【００６８】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＩＣＥ用マイコン１が、ＰＣ３から入力されたパスワードと予め保持するパスワードとを比較し、その比較結果に応じてＩＣＥ用マイコン１またはＩＣＥ２の動作を制限するようにしたので、セキュリティを向上させることが可能になると共に、利用者の利便性を向上させることが可能となった。

【００６９】

（第９の実施の形態）

本発明の第９の実施の形態におけるプログラム開発システムは、第４～第８の実施の形態におけるプログラム開発システムと比較して、一定時間毎に認証を行う点を除いて同様である。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００７０】

たとえば、第４の実施の形態におけるプログラム開発システムにおいて、ＩＣＥ用マイコン１とＩＣＥ本体２１との認証が確認された後、ＩＣＥ本体２１が別の装置に摩り替えられた場合でもＩＣＥ用マイコン１はそのまま動作を続けるので、利用権限のない者であってもＩＣＥ２を用いたプログラムのデバッグや解析が可能になる。これを防止するために、ＩＣＥ用マイコン１およびＩＣＥ本体２

１は一定時間毎に認証を行なうものである。

【００７１】

また、送受信されるコマンドやレスポンスに署名データを付加するようにすれば、装置の摩り替えを防止することができる。この場合、署名データの生成方法として、通信データを圧縮した後認証データで暗号化を行なえばよい。通信データの圧縮には、たとえばハッシュ関数などが利用できる。また、通信データを圧縮せずにそのまま暗号化してもよい。

【００７２】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、一定時間毎に再認証を行なうようにしたので、装置の摩り替えを防止することが可能となった。

【００７３】

（第１０の実施の形態）

図１５は、本発明の第１０の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、ＰＣ３と、ネットワーク５を介してＰＣ３に接続されるＩＣＥ本体２１と、ＰＯＤ２２と、ターゲットボード４とを含む。

【００７４】

ＩＣＥ本体２１を用いてプログラムをデバッグする場合、ＰＣ３からＩＣＥ本体２１にプログラムをダウンロードする必要がある。情報セキュリティマイコンのプログラムは機密性が高いため、ＩＣＥ本体２１にダウンロードするプログラムが外部に漏れると、情報セキュリティマイコンを搭載したシステムの偽造などに用いられることが想定される。

【００７５】

ＰＣ３とＩＣＥ本体２１とが１対１で接続される場合はプログラムが傍受される危険性は少ないが、ＰＣ３とＩＣＥ本体２１とがＬＡＮ（Local Area Network）などのネットワーク５によって接続される場合にはプログラムが傍受される危険性が高くなる。これを防止するために、本実施の形態においては通信データを暗号化するものである。

【００７６】

たとえば、ＰＣ３とＩＣＥ本体２１との認証を行なう際に使用された認証データおよび暗号機能を用いて通信データ（プログラム）を暗号化し、ＩＣＥ本体２１にダウンロードする。そして、ＩＣＥ本体２１は、同じ認証データを用いて復号を行なってプログラムをメモリ１２に格納する。また、通信用として認証用と別の認証データ（暗号鍵）および暗号機能を用いるようにしてもよい。

【００７７】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ＰＣ３が通信データを暗号化してＩＣＥ本体２１にダウンロードするようにしたので、ネットワークを介して通信データが傍受される危険性を少なくすることが可能となった。

【００７８】

（第１１の実施の形態）

第１～第３の実施の形態において説明したＩＣＥ用マイコン１は、システムなどに組込まれる一般の情報セキュリティマイコンとして使用できる場合がある。

【００７９】

図１６は、ＩＣＥモード（デバッグモード）と一般モードとを切替えて動作するＩＣＥ用マイコンの構成例を示す図である。図１６の上図に示すように、ＩＣＥモードで動作する場合には、ＩＣＥインタフェース１５およびＩＣＥ機能プログラム（認証プログラム、認証データを含む。）１８が動作するように制御される。なお、ＩＣＥ機能プログラム１８は、マスクＲＯＭ（Read Only Memory）、ＯＴＰＲＯＭ（One Try Programmable ROM）などに格納される。

【００８０】

また、図１６の下図に示すように、一般モードで動作する場合には、ＩＣＥインタフェース１５およびＩＣＥ機能プログラム１８が動作しないように制御される。なお、図１６の上図が実際のＩＣＥ用マイコンの構成であり、図１６の下図が一般モードのときに設定される仮想上の構成である。

【００８１】

このようにＩＣＥ用マイコン１がどちらにも使用できる場合には、ＩＣＥモー

ドと一般モードとを有しており、モードを切替えて使用されることが多い。すなわち、ＩＣＥモードで動作するプログラムを削除すれば、一般の情報セキュリティマイコンとして使用できるため、情報セキュリティマイコンの偽造に使用される危険性がある。

【００８２】

本実施の形態においては、ＩＣＥモードで動作するプログラムを削除できない構造にするか、ＩＣＥモードに固定して一般モードにならないようにすることによって、ＩＣＥ用マイコン１が一般の情報セキュリティマイコンとして使用できないようにするものである。

【００８３】

図１７は、本発明の第１１の実施の形態におけるＩＣＥ用マイコンのモードロック回路の一例を示す図である。このモードロック回路は、ＯＲ回路３１と、ヒューズ３２とを含む。一般の情報セキュリティマイコンとして出荷する場合には、ヒューズ３２をそのままにする。これによって、ＯＲ回路３１は、モード切替え信号をそのまま出力するようになる。また、一般モードに固定されるようにしてもよい。

【００８４】

ＩＣＥ用マイコン１として出荷する場合には、ヒューズ３２を切る。これによって、ＯＲ回路３１は、モード切替え信号にかかわらずハイレベルを出力して、ＩＣＥモードに固定される。すなわち、一般の情報セキュリティマイコンとして使用できなくなる。

【００８５】

図１８は、本実施の形態におけるＩＣＥ用マイコンのモードロック回路の他の一例を示す図である。このモードロック回路は、ＯＲ回路４１と、ロックコード検出回路４２とを含む。ロックコード検出回路４２は、不揮発メモリ１３の所定アドレスに書込まれているデータを読出し、そのデータがロックコードと一致する場合にはハイレベルを出力する。また、そのデータがロックコードと一致しない場合にはロウレベルを出力する。

【００８６】

一般の情報セキュリティマイコンとして出荷する場合には、不揮発メモリ１３の所定アドレスにロックコード以外のデータを書込む。これによって、ＯＲ回路４１は、モード切替え信号をそのまま出力するようになる。また、一般モードに固定されるようにしてもよい。

【００８７】

ＩＣＥ用マイコン１として出荷する場合には、不揮発メモリ１３の所定アドレスにロックコードを書込む。これによって、ＯＲ回路４１は、モード切替え信号にかかわらずハイレベルを出力して、ＩＣＥモードに固定される。すなわち、一般の情報セキュリティマイコンとして使用できなくなる。

【００８８】

以上説明したように、本実施の形態におけるＩＣＥ用マイコン１によれば、モードロック回路によってモードをＩＣＥモードに固定できるようにしたので、ＩＣＥ用マイコン１を一般の情報セキュリティマイコンとして使用できなくなり、情報セキュリティマイコンの偽造に使用される危険性を少なくすることが可能となった。

【００８９】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【００９０】

【発明の効果】

本発明のある局面によれば、認証手段によって外部機器の認証が確認されなかった場合には、プロセッサが情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるので、使用権限がない者が情報セキュリティマイクロコンピュータをＩＣＥ用マイコンとして利用することができなくなり、セキュリティを向止させることが可能となった。

【００９１】

本発明の別の局面によれば、本体と情報セキュリティマイクロコンピュータと

の間で認証を行ない、認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるので、使用権限がない本体が情報セキュリティマイクロコンピュータをＩＣＥ用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となった。

【００９２】

本発明のさらに別の局面によれば、情報セキュリティマイクロコンピュータ、本体およびコンピュータのうち、少なくともいずれか２つの間で認証を行なうので、使用権限がない本体またはコンピュータが情報セキュリティマイクロコンピュータをＩＣＥ用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となった。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態におけるＩＣＥ用マイコンの概略構成を示すブロック図である。

【図２】　ＩＣＥ用マイコン１とＩＣＥ本体との間の認証を説明するための図である。

【図３】　本発明の第１の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの一例を示す図である。

【図４】　ＩＣＥ２の機能的構成を示すブロック図である。

【図５】　本発明の第１の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図６】　本発明の第２の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図７】　本発明の第３の実施の形態におけるＩＣＥ用マイコン１を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図８】　本発明の第４の実施の形態におけるＩＣＥ本体２１の機能的構成を示すブロック図である。

【図９】　本発明の第５の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図１０】　本発明の第５の実施の形態におけるプログラム開発システムの

概略構成の他の一例を示すブロック図である。

【図１１】　本発明の第６の実施の形態におけるプログラム開発システムの概略構成を示すブロック図である。

【図１２】　本発明の第７の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図１３】　本発明の第８の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図１４】　本発明の第８の実施の形態におけるプログラム開発システムの処理手順を説明するためのフローチャートである。

【図１５】　本発明の第１０の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図１６】　ＩＣＥモードと一般モードとを切替えて動作するＩＣＥ用マイコンの構成例を示す図である。

【図１７】　本発明の第１１の実施の形態におけるＩＣＥ用マイコンのモードロック回路の一例を示す図である。

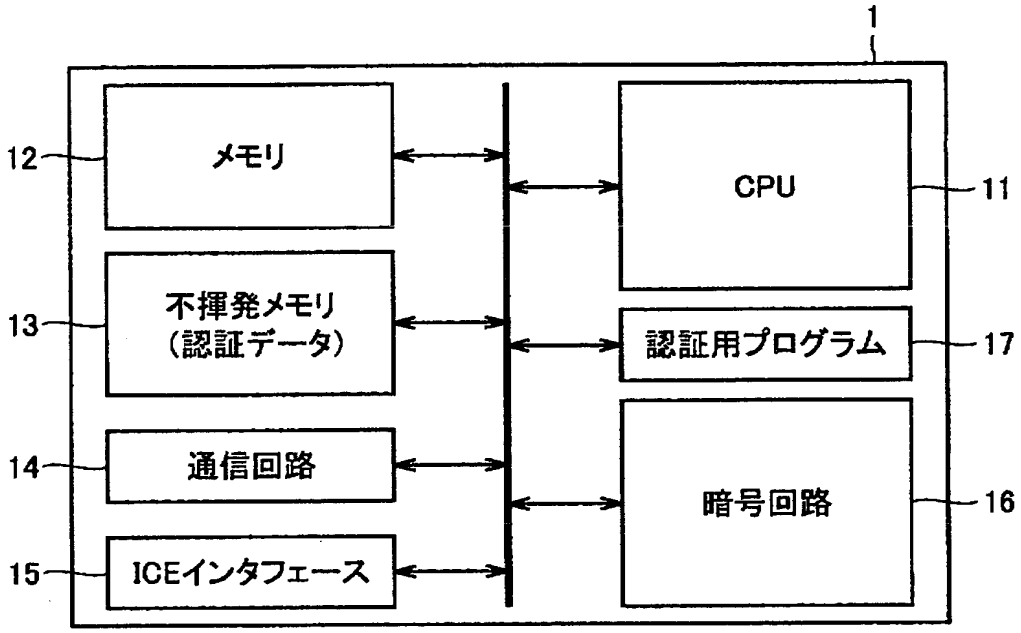
【図１８】　本発明の第１１の実施の形態におけるＩＣＥ用マイコンのモードロック回路の他の一例を示す図である。

【符号の説明】

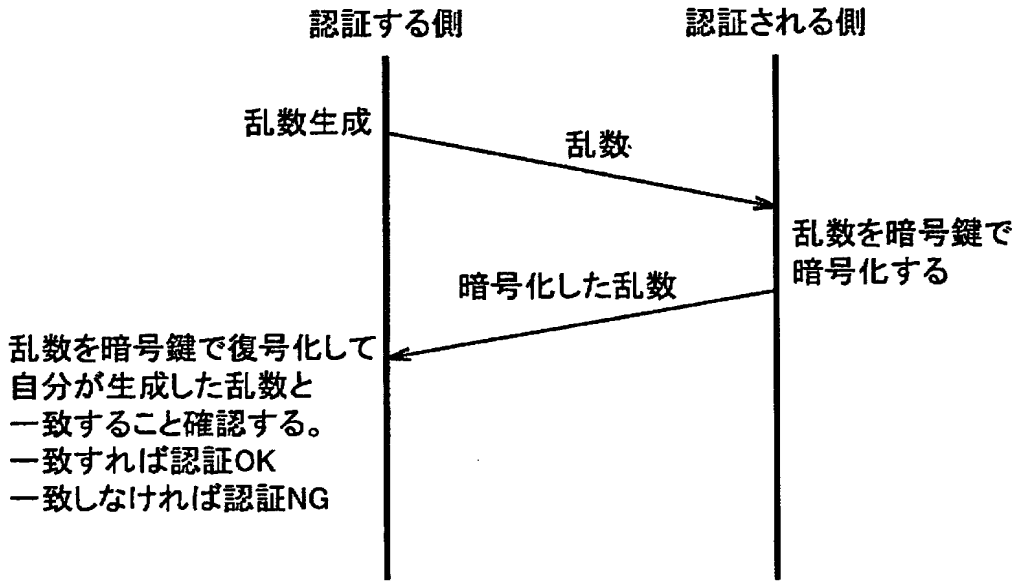
１　ＩＣＥ用マイコン、２　ＩＣＥ、３　ＰＣ、４　ターゲットボード、５　ネットワーク、１１　ＣＰＵ、１２　メモリ、１３　不揮発メモリ、１４　通信回路、１５　ＩＣＥインタフェース、１６　暗号回路、１７，２１２　認証用プログラム、１８　ＩＣＥ機能プログラム、２１　ＩＣＥ本体、２２　ＰＯＤ、３１，４１　ＯＲ回路、３２　ヒューズ、４２　ロックコード検出回路、２１１　ＩＣＥ制御部、２１３　認証データ。

【書類名】　　図面

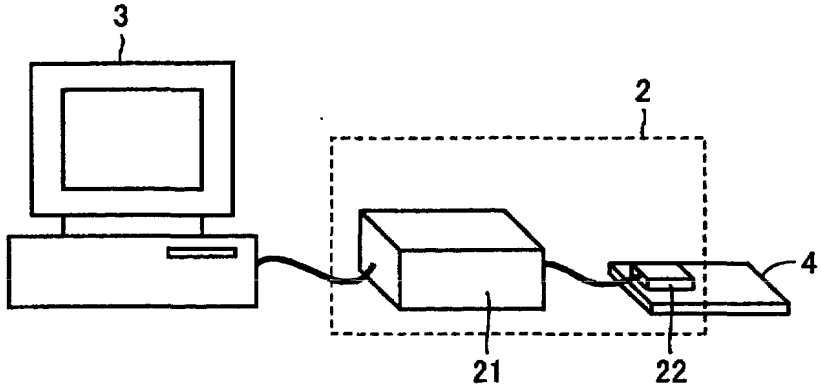
【図１】


1
12
メモリ
CPU
11
13
不揮発メモリ
（認証データ）
認証用プログラム
17
14
通信回路
暗号回路
16
15
ICEインタフェース

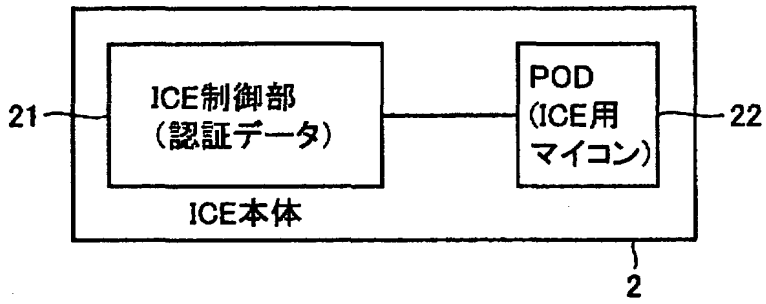
【図２】


認証する側
認証される側
乱数生成
乱数
乱数を暗号鍵で
暗号化する
暗号化した乱数
乱数を暗号鍵で復号化して
自分が生成した乱数と
一致すること確認する。
一致すれば認証OK
一致しなければ認証NG

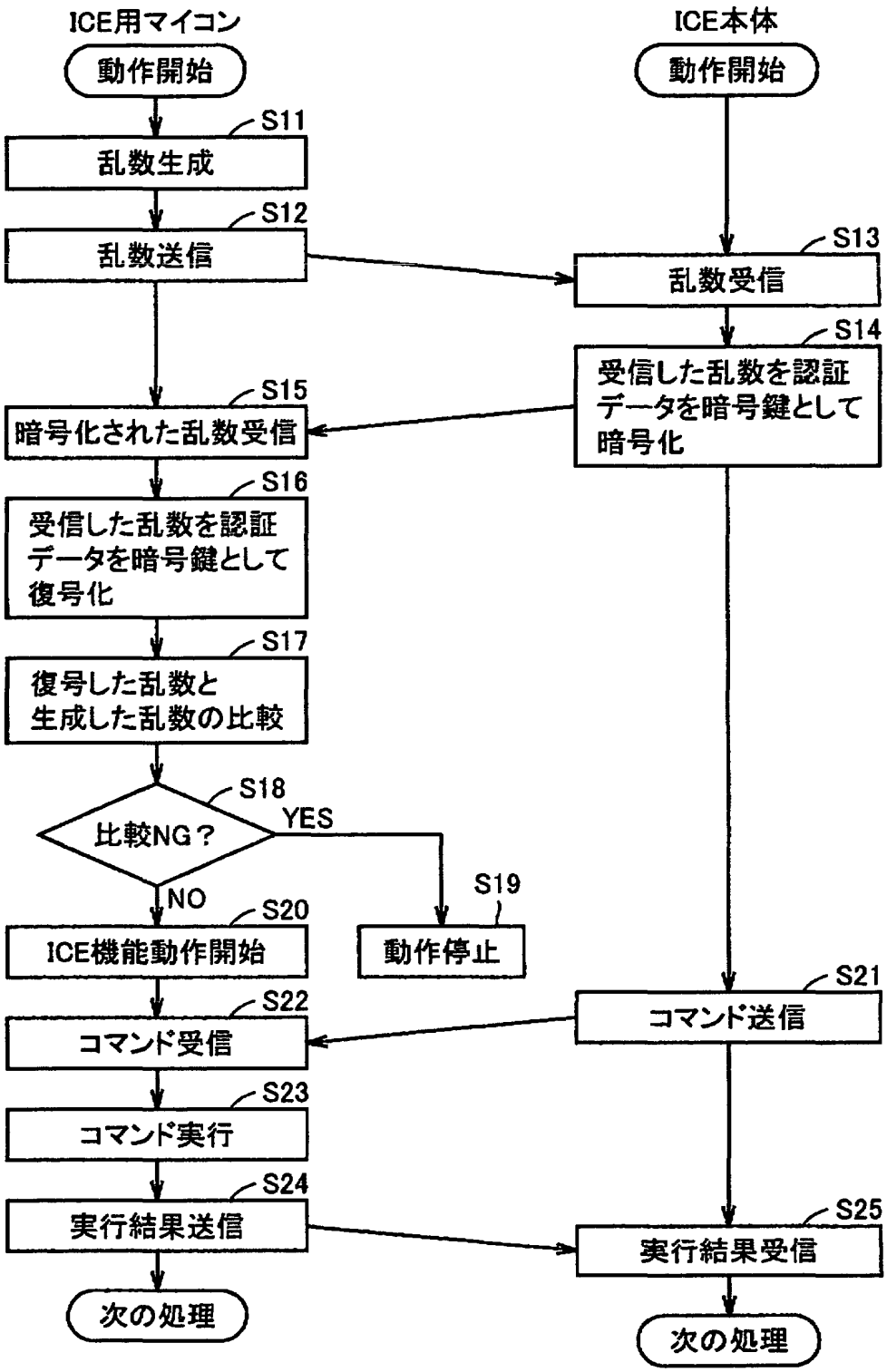
【図３】



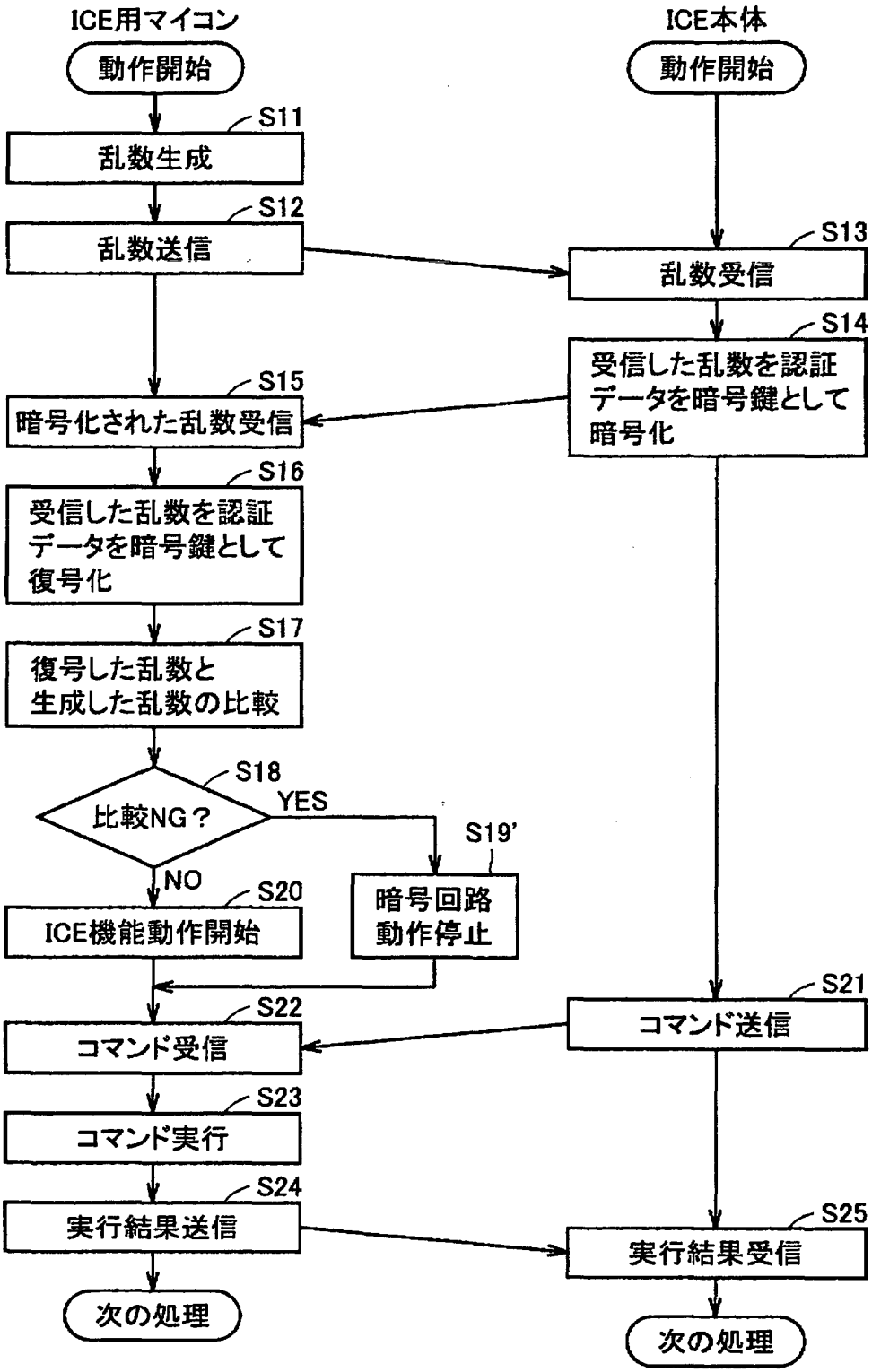

【図４】



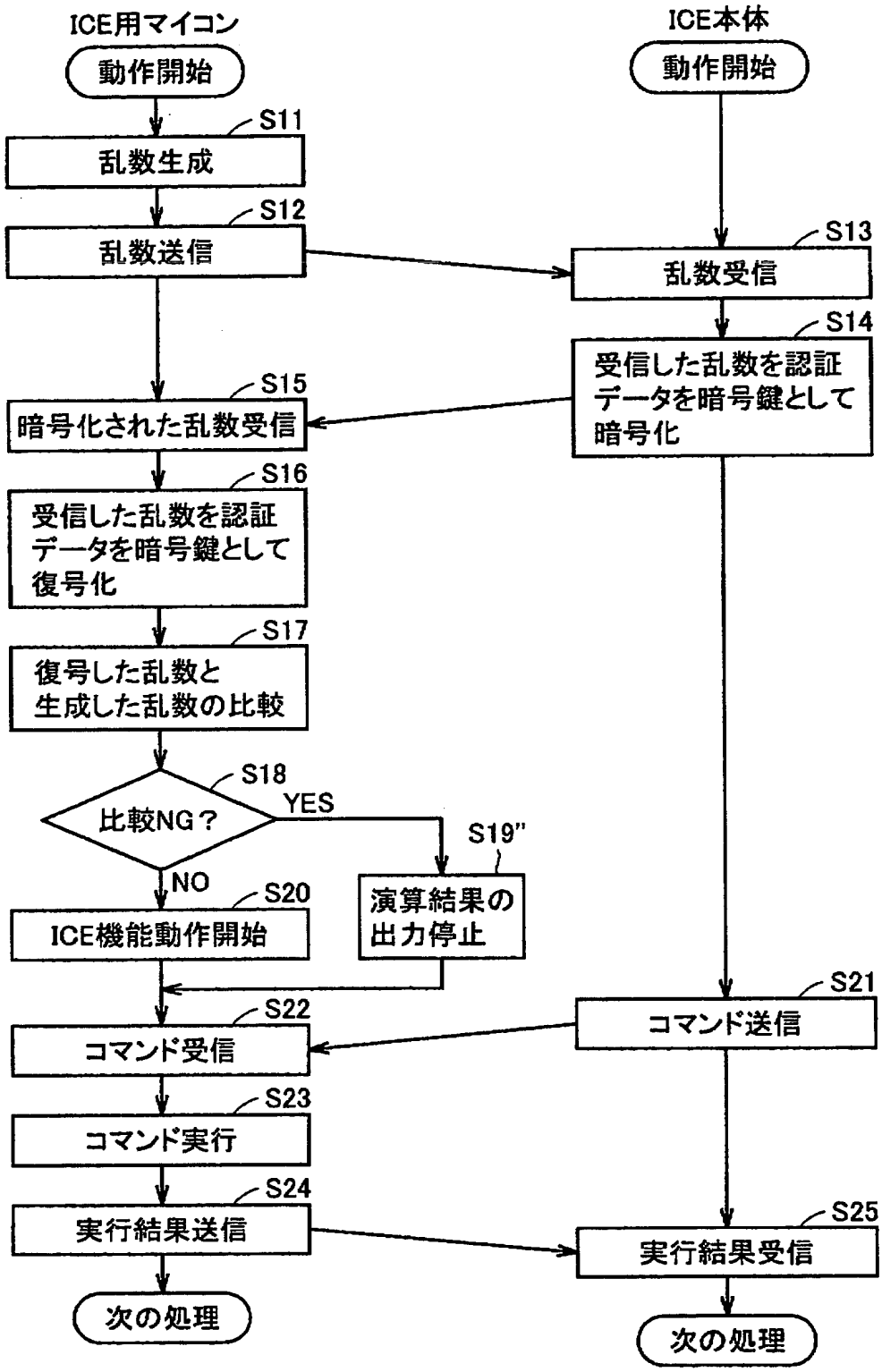
【図５】


ICE用マイコン
動作開始
S11
乱数生成
S12
乱数送信
S15
暗号化された乱数受信
S16
受信した乱数を認証データを暗号鍵として復号化
S17
復号した乱数と生成した乱数の比較
S18
比較NG？
YES
NO
S19
動作停止
S20
ICE機能動作開始
S22
コマンド受信
S23
コマンド実行
S24
実行結果送信
次の処理
ICE本体
動作開始
S13
乱数受信
S14
受信した乱数を認証データを暗号鍵として暗号化
S21
コマンド送信
S25
実行結果受信
次の処理

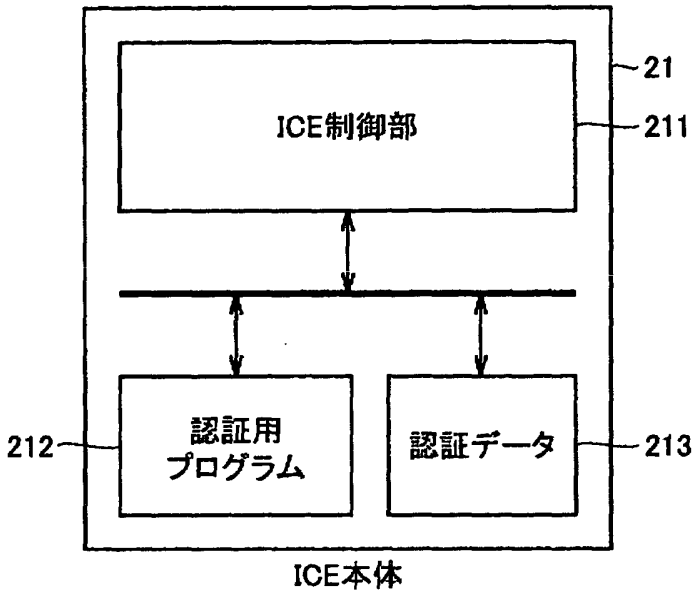
【図６】


ICE用マイコン
動作開始
S11
乱数生成
S12
乱数送信
S15
暗号化された乱数受信
S16
受信した乱数を認証データを暗号鍵として復号化
S17
復号した乱数と生成した乱数の比較
S18
比較NG？
YES
S19'
暗号回路動作停止
NO
S20
ICE機能動作開始
S22
コマンド受信
S23
コマンド実行
S24
実行結果送信
次の処理
ICE本体
動作開始
S13
乱数受信
S14
受信した乱数を認証データを暗号鍵として暗号化
S21
コマンド送信
S25
実行結果受信
次の処理

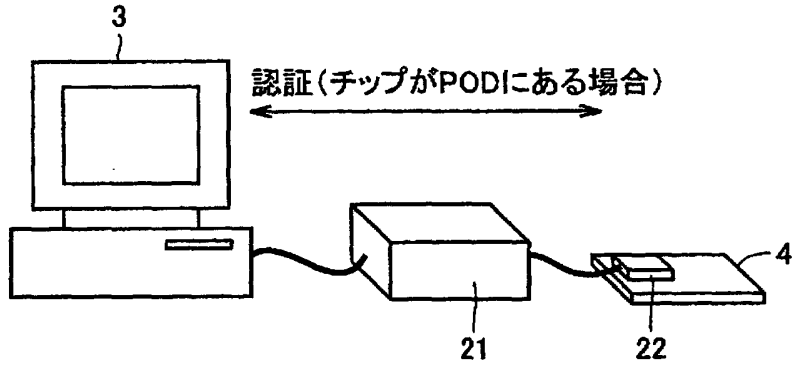
【図７】


ICE用マイコン
動作開始
S11
乱数生成
S12
乱数送信
S15
暗号化された乱数受信
S16
受信した乱数を認証データを暗号鍵として復号化
S17
復号した乱数と生成した乱数の比較
S18
比較NG？
YES
S19"
演算結果の出力停止
NO
S20
ICE機能動作開始
S22
コマンド受信
S23
コマンド実行
S24
実行結果送信
次の処理
ICE本体
動作開始
S13
乱数受信
S14
受信した乱数を認証データを暗号鍵として暗号化
S21
コマンド送信
S25
実行結果受信
次の処理

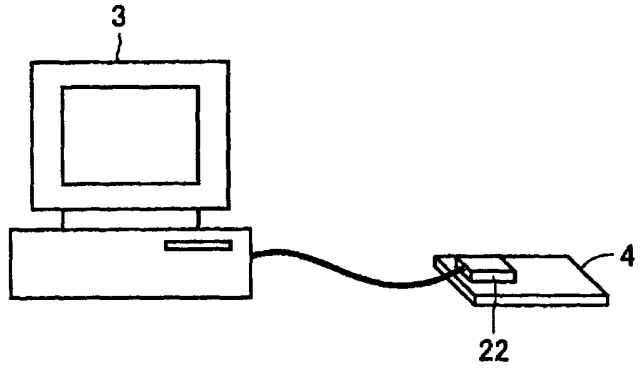
【図８】


21
ICE制御部
211
212
認証用
プログラム
認証データ
213
ICE本体

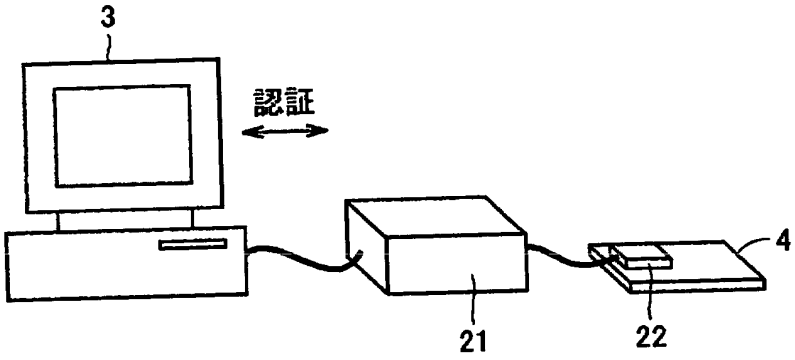
【図９】


3
認証（チップがPODにある場合）
4
21
22

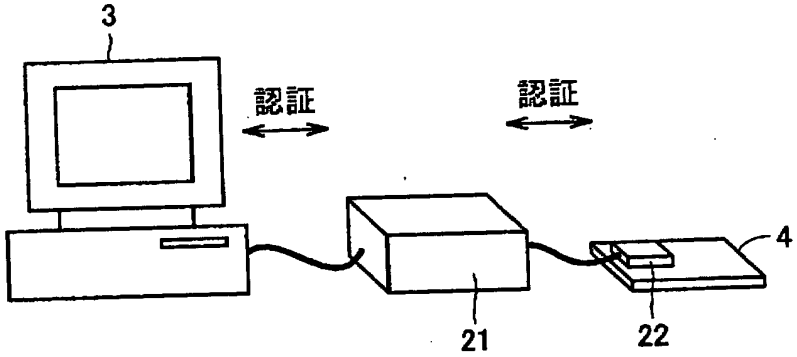
【図１０】


3
4
22

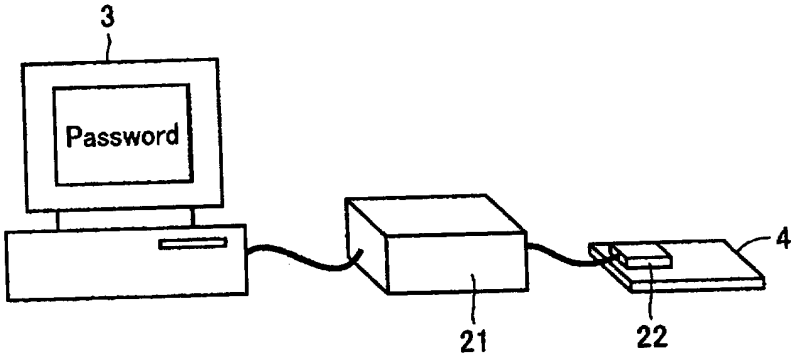
【図１１】



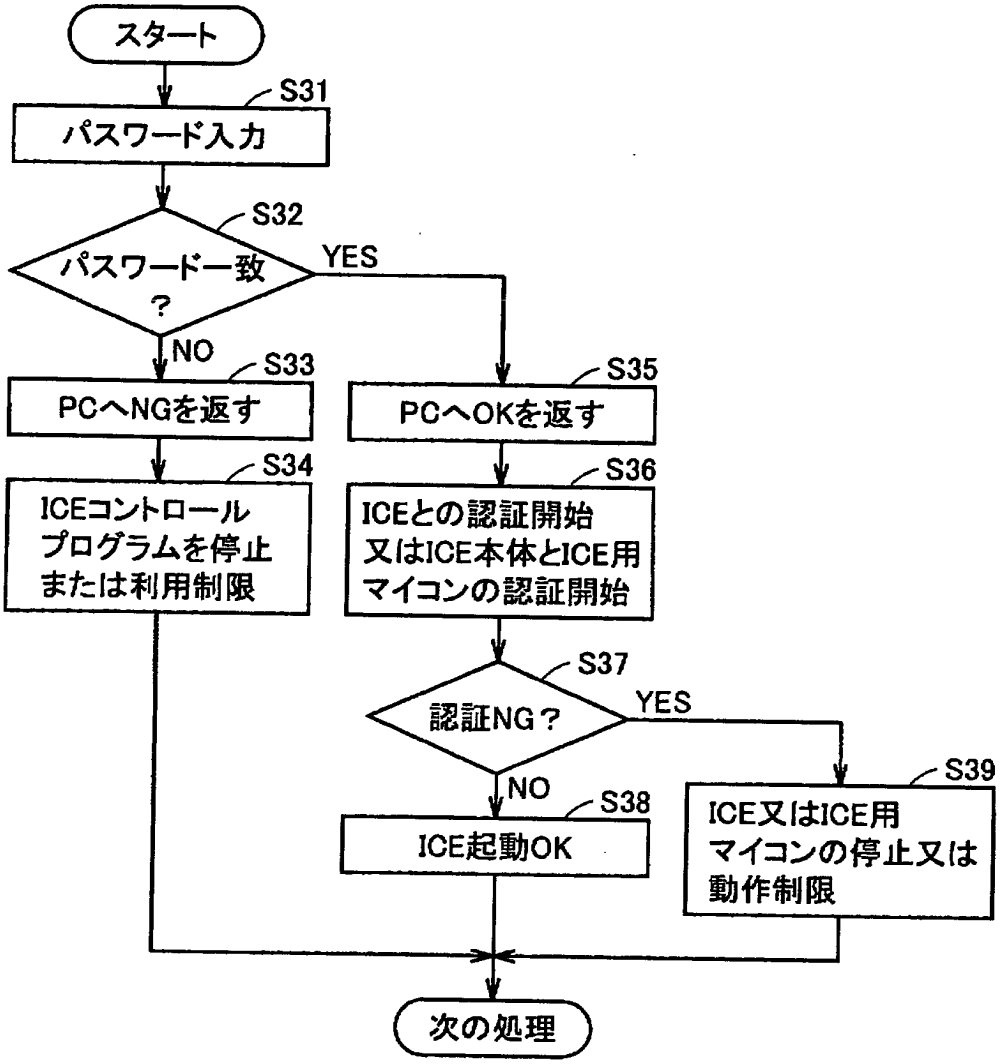

【図１２】



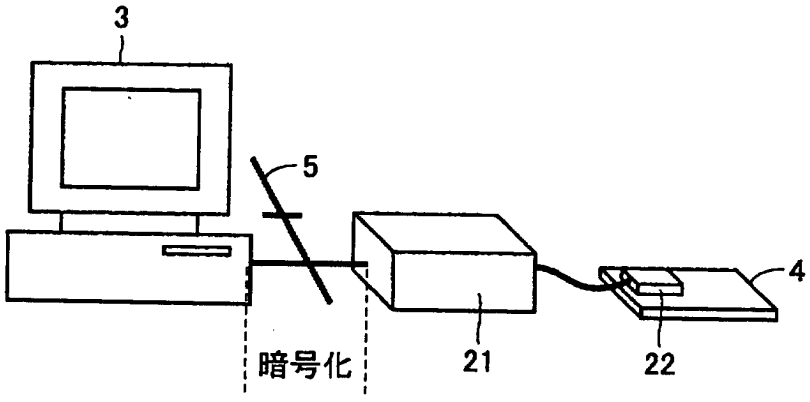

【図１３】



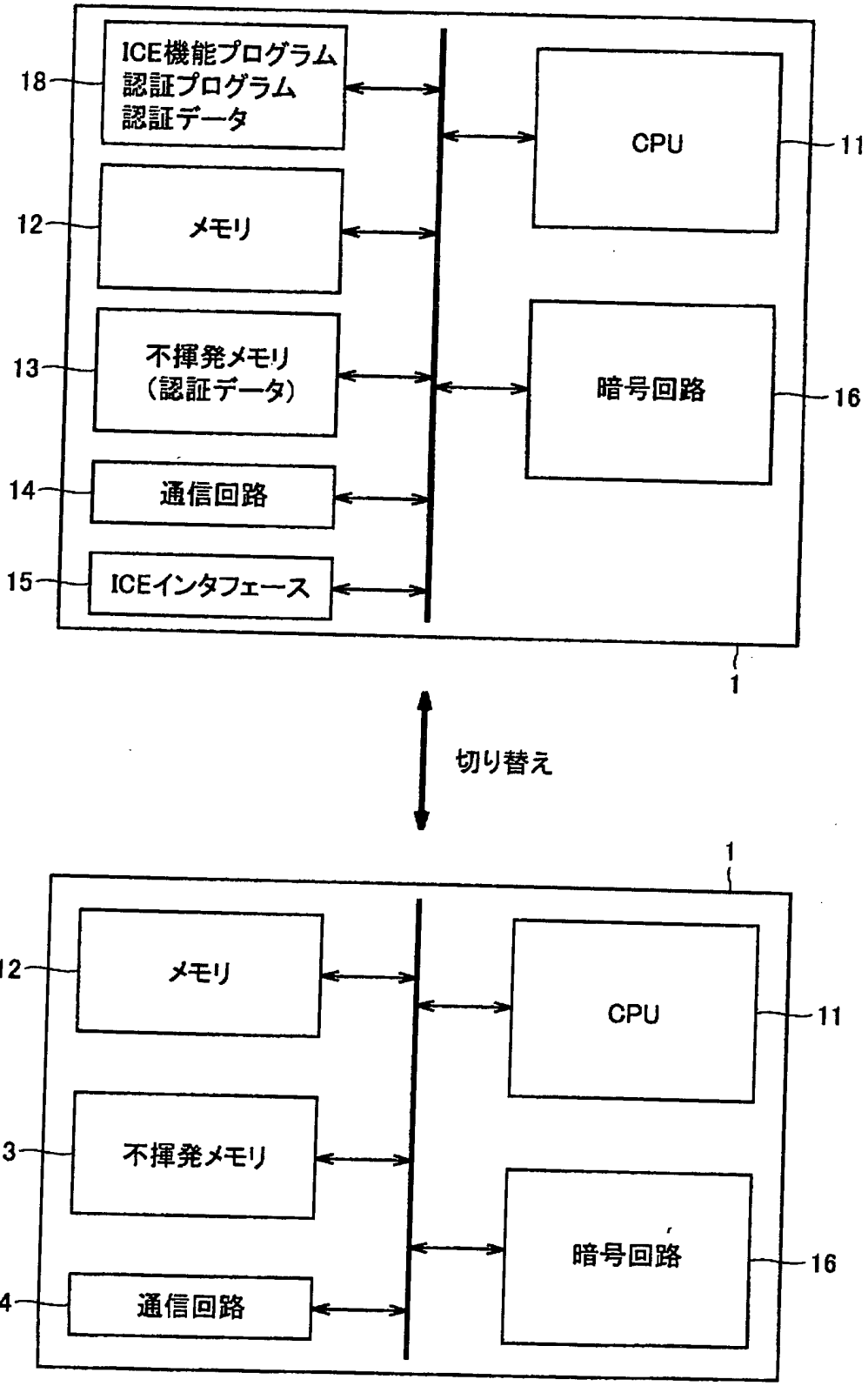
【図１４】


スタート
S31
パスワード入力
S32
パスワード一致？
YES
NO
S33
PCへNGを返す
S34
ICEコントロールプログラムを停止または利用制限
S35
PCへOKを返す
S36
ICEとの認証開始又はICE本体とICE用マイコンの認証開始
S37
認証NG？
YES
NO
S38
ICE起動OK
S39
ICE又はICE用マイコンの停止又は動作制限
次の処理

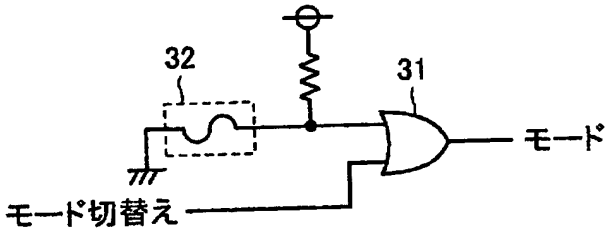
【図１５】


3
5
4
暗号化
21
22

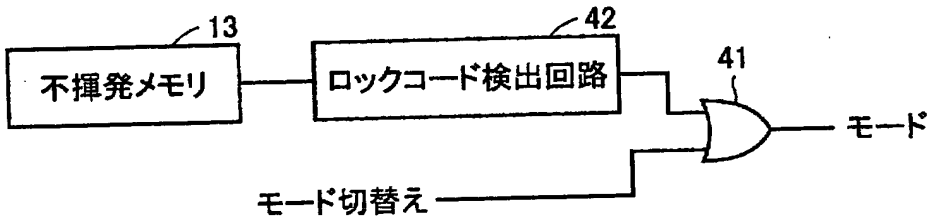
【図１６】


ICE機能プログラム
認証プログラム
認証データ
18
CPU
11
メモリ
12
不揮発メモリ
（認証データ）
13
暗号回路
16
通信回路
14
ICEインタフェース
15
1
切り替え
1
メモリ
12
CPU
11
不揮発メモリ
13
暗号回路
16
通信回路
14

【図１７】




【図１８】



【書類名】　　要約書

【要約】

【課題】　使用権限がない者がＩＣＥ用マイコンとして利用することが不可能な情報セキュリティマイクロコンピュータを提供すること。

【解決手段】　情報セキュリティマイクロコンピュータ１は、情報の暗号化および復号を行なう暗号回路１６と、ＩＣＥ本体の認証を行なう認証用プログラム１７と、情報セキュリティマイクロコンピュータ１の全体的な制御を行なうＣＰＵ１１とを含む。ＣＰＵ１１は、ＩＣＥ本体の認証が確認されなかった場合には、情報セキュリティマイクロコンピュータ１の少なくとも一部の機能を停止させる。したがって、使用権限がない者が情報セキュリティマイクロコンピュータ１をＩＣＥ用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となる。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社

# 出　願　人　履　歴　情　報

識別番号　　〔３９１０２４５１５〕

１．変更年月日　　１９９７年１１月２６日
［変更理由］　名称変更
住　所　兵庫県伊丹市中央３丁目１番１７号
氏　名　三菱電機システムエル・エス・アイ・デザイン株式会社